Многочлены над полем $\mathbb{F}_p$

Пусть p — простое число. Обозначим через $\mathbb{F}_p$ множество (поле) остатков от деления на p. Через $0 \in \mathbb{F}_p$ будем обозначать нулевой остаток. Множество $\mathbb{F}_p$ состоит из p элементов, которые можно умножать, складывать и вычитать. Более того, любой элемент $a \in \mathbb{F}_p$ можно поделить на любой $0 \neq b \in \mathbb{F}_p$. Сложение и умножение являются *ассоциативными* и *коммутативными* операциями, *дистрибутивность* также выполняется.

Многочленом $P(x)$ с коэффициентами в $\mathbb{F}_p$ назовем формальное выражение $P(x) = a_0 + a_1x + \ldots + a_kx^k + \ldots$, где x — формальная переменная, $a_0, \ldots, a_k, \ldots \in \mathbb{F}_p$ и только конечное число a_i ненулевые. Многочлены можно складывать и умножать, как обычно:

$$(a_0 + \ldots + a_kx^k + \ldots) \pm (b_0 + \ldots + b_kx^k + \ldots) = (a_0 \pm b_0) + (a_1 \pm b_1)x + \ldots + (a_k \pm b_k)x^k + \ldots$$

$$(a_0 + \ldots + a_kx^k + \ldots) \cdot (b_0 \ldots + b_kx^k + \ldots) = (a_0 \cdot b_0) + (a_1b_0 + a_0b_1)x + \ldots$$
$$\ldots + (a_kb_0 + a_{k-1}b_1 + \ldots + a_0b_k)x^k + \ldots$$

Часто для краткости мы будем пропускать нулевые слагаемые и записывать многочлены в виде

$$P(x) = a_0 + a_1x + \ldots + a_nx^n.$$

Множество многочленов с коэффициентами в $\mathbb{F}_p$ мы будем обозначать через $\mathbb{F}_p[x]$.

Степенью многочлена $P(x) = a_0 + a_1x + \ldots + a_kx^k + \ldots$ называется наибольшее целое d такое, что $a_d \neq 0$. Будем обозначать ее через $\deg P(x)$. У нулевого многочлена степень не определена.

Многочлены $P(x) \in \mathbb{F}_p[x]$ можно вычислять на остатках. Иными словами, если $P(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{F}_p[x]$ и $c \in \mathbb{F}_p$ — остаток, то $P(c) = a_0 + a_1c + \ldots + a_nc^n \in \mathbb{F}_p$ — также остаток.

$\boxed{1}$ Для многочленов $P(x), Q(x) \in \mathbb{F}_p[x]$ докажите, что

(a) $\deg(P(x) + Q(x)) \leq \max(\deg P(x), \deg Q(x))$;

(b) $\deg(P(x) \cdot Q(x)) = \deg P(x) + \deg Q(x)$.

$\boxed{2}$ Пусть $P(x), Q(x) \in \mathbb{F}_p[x]$. Докажите по индукции по $\deg P(x)$, что многочлен $P(x)$ можно поделить на $Q(x)$ с остатком. А именно, что существуют многочлены $S(x), R(x) \in \mathbb{F}_p[x]$ такие, что $\deg R(x) < \deg Q(x)$ и $P(x) = Q(x)S(x) + R(x)$.

$\boxed{3}$ Поделите с остатком многочлен $P(x)$ на $Q(x)$ в случае

(a) $P(x), Q(x) \in \mathbb{F}_{13}[x] : P(x) = x^7, Q(x) = x^2 - 1$

(b) $P(x), Q(x) \in \mathbb{F}_{11}[x] : P(x) = x^3, Q(x) = 6x^2 + x + 1$

(c) $P(x), Q(x) \in \mathbb{F}_7[x] : P(x) = x^7 + 2x + 1, Q(x) = x - 3$

$\boxed{4}$ **Теорема Безу.** Дан остаток $a \in \mathbb{F}_p$. Докажите, что многочлен $P(x) \in \mathbb{F}_p[x]$ даёт остаток $P(a)$ при делении на $x - a$.

$\boxed{5}$ Дан остаток $a \in \mathbb{F}_p$. Докажите, что многочлен $P(x) \in \mathbb{F}_p[x]$ делится на $x - a$ тогда и только тогда, когда a является его корнем, то есть остаток $P(a)$ — нулевой.

$\boxed{6}$ (a) Пусть $a_1, \ldots, a_k$ — различные остатки. Докажите, что многочлен $P(x) \in \mathbb{F}_p[x]$ делится на произведение $(x - a_1) \cdot \ldots \cdot (x - a_k)$ тогда и только тогда, когда все a_i являются корнями $P(x)$.

(b) Докажите, что у многочлена степени $n > 0$ над $\mathbb{F}_p$ не более n различных корней.

$\boxed{7}$ Разложите на множители многочлены:

(a) $x^p - x \in \mathbb{F}_p[x]$;

(b) $x^p - 2 \in \mathbb{F}_p[x]$;

(c) $1 + x + \ldots + x^{p-1} \in \mathbb{F}_p[x]$.

$\boxed{8}$ **Теорема Виета.** Пусть различные остатки $a_1, \ldots, a_n$ — корни многочлена $b_n x^n + \ldots + b_1 x + b_0$. Докажите, что

$$\begin{aligned} a_1 + \ldots + a_n &= -\frac{b_{n-1}}{b_n}, \\ a_1 a_2 + a_1 a_3 + \ldots + a_{n-1} a_n &= \frac{b_{n-2}}{b_n}, \\ &\vdots \\ a_1 a_2 \ldots a_n &= (-1)^n \frac{b_0}{b_n}. \end{aligned}$$

$\boxed{9}$ Петя выписал в тетрадку все наборы из трёх натуральных чисел $1 \leq k \leq p$. Затем он перемножил числа в каждой тройке, а результаты сложил. Какой остаток даёт получившееся число при делении на p?